



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1500  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/629,599	07/30/2003	Antonio Lain	200205658-2	6218

22879 7590 03/13/2007  
HEWLETT PACKARD COMPANY  
P O BOX 272400, 3404 E. HARMONY ROAD  
INTELLECTUAL PROPERTY ADMINISTRATION  
FORT COLLINS, CO 80527-2400

EXAMINER
----------

KOEMPEL THOMAS, BEATRICE L

ART UNIT	PAPER NUMBER
----------	--------------

2132

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/13/2007	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	Application No. 10/629,599	Applicant(s) LAIN ET AL.	
	Examiner Bea Koempel-Thomas	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 17 January 2007.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1,2 and 4-21 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,2 and 4-21 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 17 January 2007 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

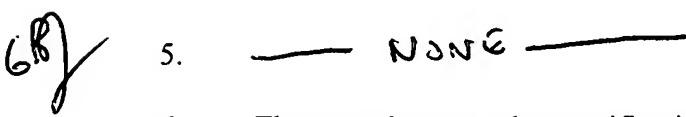
- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

**DETAILED ACTION**

1. Previously presented claims 1, 2 and 4-13 are pending in this application.
2. Claim 3 was cancelled by the amendment filed 17 January 2007.
3. Claims 14-21 have been presented in the amendment filed 17 January 2007.
4. Claims 1, 2 and 4-21 are pending in this application and presented for examination.
5.  NONE
6. The amendment to the specification filed 17 January 2007, is accepted.
7. The amendment of the drawings, Figure 1, filed 17 January 2007, is accepted by the examiner as understood to present reference characters (10 for the server) and (20 for the clients C1) as supported by the specification (p. 4 ll. 8-10); Please amend the "Amendments to the Drawings," page 10 of the response filed 17 January 2007, to reflect the applicant's intended amendment regarding "clients C1."
8. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office Action.
9. Below, Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully

Art Unit: 2132

requested from the applicant, in preparing the response, to consider fully each reference in its entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

***Response to Remarks***

10. Applicant's remarks filed 17 January 2007, have been fully considered but they are not fully persuasive.

11. Applicant's arguments with respect to claim 1 being unpatentable under 35 U.S.C. 112, second paragraph, as amended, have been fully considered and are persuasive. The rejection of claim 1 under 35 U.S.C. 112, second paragraph has been withdrawn.

12. Applicant's arguments with respect to claim 1 being unpatentable under 35 U.S.C. 103, as amended, have been considered but are moot in view of the new ground(s) of rejection, below.

13. The rejection of claims 10-12 under 35 U.S.C. 103, as being obvious over Sweet in view of Stefik '971, is maintained. These rejections are maintained because the amendments neither overcome the rejection nor necessitate citation of additional prior art references. The only difference that examiner recognizes between original claim 1 and claims 10-12 as rejected is that claim 1 is directed toward managing keys, and claims 10-12 are directed toward managing providing keys. While the limitations are not linguistically identical, they are each covered by the cited prior art references.

For example, and to further clarify the rejections, regarding claim 10: Sweet discloses managing providing security keys to users, generating security keys, issuing security keys, and monitoring user status ([0023] "key management," [0025] access permission credentials, and

Art Unit: 2132

[0037] distributing working keys). Stefik '971 discloses another approach to managing providing security keys to users, generating security keys, issuing security keys, monitoring user status, and a policy resulting in economic disbenefit for misuse of the service (col. 15-16 ll. 5-31, master repository issues certificates and maintains encryption keys; level 5 repository erases digital identifiers and modifies certificates to indicate system compromised; destruction of digital identity would effect an economic penalty).

Additionally, to further clarify the rejections, regarding claims 11 and 12: Stefik '971 discloses a decision process for invalidating a security key, and such an aggregated decision process (col. 15-16 ll. 5-31, assignment of individual works to chosen repository levels aggregates such decision making, indicates the value of such works, and commands the attendant results of system compromise regarding such works including destruction of digital identities).

As discussed in the office action filed 18 October 2006: It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the apparatus taught by Sweet with the technology of Stefik '971, in order to assure the convenience of access and low-overhead billing, despite some unauthorized copying (*see* Stefik '971, col. 15 ll. 18-24). Furthermore, such a person would have been motivated to make such a combination to enable a system that provides for remuneration for all copies made of high value works (*see* Stefik '971, col. 3-4 ll. 64-4).

14. The rejection of claims 4-6 under 35 U.S.C. 103, as being obvious over the combination of Sweet and Stefik '971 in view of Stefik '392 is maintained. **In response to applicant's**

**amendment of the claims, and to further clarify prosecution, examiner has consolidated all Stefik references to refer to Stefik '971.**

The rejection is maintained regarding claim 4, because: the combination of Sweet and Stefik '971 discloses the method of claim 1, (discussed below). Furthermore, and to further clarify the rejection, Stefik '392 as originally cited, and Stefik '971, teach a value aggregating the economic penalty for system compromise via the assignment of works to chosen repository levels (col. 15-16 ll. 5-31, see rejection of claim 12).

The rejection is maintained regarding claim 5, for the same reasons as claims 1 and 4, and to further clarify, because Stefik '392 as originally cited, and Stefik '971 disclose controlling access to digital works and billing for all uses of copies of works, which reasonably includes dilution of the economic value to an authorized user for provision to an unauthorized user; for example, erasing the content of the designated document (col. 6-7 ll. 66-14 and col. 15-16 ll. 5-24).

The rejection is maintained regarding claim 6, for the same reasons as claim 1, and to further clarify, because Stefik '392 as originally cited, and Stefik '971 disclose user interfaces and credit servers which interact to charge and process fees associated with exercising rights; a variety of rights are possible through the use of a flexible and extensible usage rights language, which reasonably includes forwarding the cost of arising from providing network and server capacity to unauthorized users (col. 6-7 ll. 66-14 and col. 15-18 ll. 5-10).

Art Unit: 2132

15. **The rejection of claims 2, 7-9 and 13 under 35 U.S.C. 103, as being obvious over the combination of Sweet and Stefik '971 further in view of Aiello et al., U.S. Patent No. 6,397,329 B1, (hereinafter "Aiello"), is maintained.**

These rejections are maintained at least for the same reasons as the rejections of independent claims 1 and 10, and additionally because the amendments neither overcome the rejections nor necessitate citation of additional prior art references. As originally cited, Aiello cures any deficiencies that Sweet or Stefik '971, may have regarding these claims.

#### ***Claim Objections***

16. Claim 1 as amended, is objected to because of the following informality: "if the second **valid** does not exceed," (4<sup>th</sup> line from the bottom), appears to include a typographical error. In order to further prosecution, examiner interpreted "valid" as "value." Appropriate correction is required.

17. Claim 15 is objected to because of the following informality: grammatical error, line 3, "comprising" interpreted as "comprises" in order to further prosecution. Appropriate correction is required.

18. Claim 21 is objected to because of the following informality: "the third cost" lacks antecedent basis. In order to further prosecution, examiner interpreted claim 21 as depending from claim 17, which provides antecedent basis for "the third cost." Appropriate correction is required.

***Claim Rejections - 35 USC § 112, first paragraph***

19. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

20. Claims 14 and 15 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The limitation “only share a first generation root key” is not supported by the disclosure (p. 7 ll. 10-11, “keys of lower generations will tend to share more common ancestor keys of higher generations,” describes multiple generations of keys and does not describe subsections only sharing first generation root keys).

***Claim Rejections - 35 USC § 112, second paragraph***

21. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

22. Claims 14 and 15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.



The phrase “a length of time subscribed **to for** the service,” renders the claims indefinite because it is unclear if the applicant intended to claim forward looking or backward looking subscription. As filed, the scope of the claimed subject matter cannot be determined.

***Claim Rejections - 35 USC § 103***

23. **Claim 1, as amended via incorporation of the limitation of former claim 3, is rejected under 35 U.S.C. 103(a) as being unpatentable over Sweet, U.S. Publication No. 2002/0031230 A1, (hereinafter “Sweet”), in view of Stefik et al., U.S. Patent No. 6,236,971, (hereinafter “Stefik ‘971”), as applied to claim 1 in the office action filed 18 October 2006. Please note the disclosure of Stefik et al., U.S. Patent No. 7,024,392 B2, (hereinafter “Stefik ‘392”) as applied to claim 3 in the same office action contains identical subject matter in this regard as Stefik ‘971.**

24. In response to applicant’s amendment of the claims, and to further clarify prosecution, examiner has consolidated all Stefik references to refer to Stefik ‘971.

25. **Regarding (currently amended) claim 1:** Sweet discloses a method of managing security keys ([0023] “key management”) provided to users of a service, the method comprising the steps of: issuing a security key to a first user eligible to receive the service ([0037] distributing working keys); and monitoring the first user's status to establish whether the first user is eligible to receive the service ([0025] access permission credentials).

Sweet does not disclose establishing, in accordance with a policy, a first value associated with invalidation of the first user's security key at a particular point in time, and a second value

Art Unit: 2132

associated with providing the service to an ineligible user at the particular point in time, and if the second value exceeds the first value, invalidating the first user's security key at the particular point in time, wherein the first user's security key is kept valid if the second value does not exceed the first value, and wherein the policy provides that the second value is related to the economic penalty associated with provision of the service to the ineligible user.

Stefik '971 discloses establishing, in accordance with a policy, a first value associated with invalidation of the first user's security key at a particular point in time, and a second value associated with providing the service to an ineligible user at the particular point in time, and if the second value exceeds the first value, invalidating the first user's security key at the particular point in time (col. 15-16 ll. 5-31, master repository issues certificates and maintains encryption keys; level 5 repository erases digital identifiers and modifies certificates to indicate system compromised),

wherein the first user's security key is kept valid if the second value does not exceed the first value (col. 15-16 ll. 5-31), and

wherein the policy provides that the second value is related to the economic penalty associated with provision of the service to the ineligible user (col. 15-16 ll. 5-31, destruction of digital identity would effect an economic penalty).

**26. Claims 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Sweet, Stefik '971 and Aiello in view of Dolphin U.S. Patent No. 5,457,746, (hereinafter "Dolphin").**

Art Unit: 2132

27. **Regarding (new) claims 14 and 15:** The combination of Sweet, Stefik '971 and Aiello discloses a method as indicated above, further comprising the step of:

assigning security keys to users (Sweet, [0033] selected groups of users to be provided keys are identified),

wherein a first set of users are assigned security keys (Sweet, [0041] groups of users are provided access codes (keys) according to each user's defined group) in a first subsection of the binary tree (Aiello, col. 8 ll. 34-44 and col. 17 ll. 10-29, two data revocation structures in a binary tree),

wherein a second set of users are assigned security keys (Sweet, [0041]) in a second subsection of the binary tree (Aiello, col. 8 ll. 34-44 and col. 17 ll. 10-29), and

wherein the security keys of the first subsection of the binary tree only share a first generation root key as a common ancestor with the security keys of the second subsection of the binary tree (Aiello, col. 8 ll. 34-44 and Abstract, each subset's certificate includes a chain including the zero token for each included chain).

The combination of Sweet, Stefik '971 and Aiello does not describe assigning security keys to users based on a length of time subscribed to for the service. Dolphin describes assigning security keys to users based on a length of time subscribed to for the service (col. 5 ll. 40-56, attributes include time of subscription).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify the combination of Sweet, Stefik '971 and Aiello by the time based subscription attributes as taught by Dolphin in order to correlate time of access with billing (*see* Dolphin, col. 2 ll. 44-67).

Art Unit: 2132

28. **Claims 16 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Sweet, Stefik '971, Stefik '392, and Aiello.**

29. **Regarding (new) claim 16:** The combination of Sweet, Stefik '971 and Stefik '392 discloses a method as indicated above, wherein security keys are ancestry based (Stefik '971, col. 11-12 ll. 59-3, usage rights are defined by those rights belonging to ancestors).

The combination of Sweet, Stefik '971 and Stefik '392 does not describe wherein the security keys are generated in an ancestry-based, binary tree hierarchy, wherein invalidation of a given key necessitates a need for reconfiguration of each key in the hierarchy, or wherein the first value is computed by adding a first cost associated with invalidating all security keys of the ineligible users, with a second cost associated with reconfiguring all security keys of eligible users that are in an ancestry chain of any one of the security keys of the ineligible users.

Aiello describes wherein the security keys are generated in a binary tree hierarchy (col. 8 ll. 52),

wherein invalidation of a given key necessitates a need for reconfiguration of each key in the hierarchy (col. 6-7 ll. 10-4, token value dependent on chain),

wherein the first value is computed by adding a first cost associated with invalidating all security keys of the ineligible users, with a second cost associated with reconfiguring all security keys of eligible users that are in an ancestry chain of any one of the security keys of the ineligible users (col. 5-7 ll. 55-63, cost of communications and network resources reduced by selected revocation and updating scheme in binary tree structure using chain of token values).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the combination of Sweet, Stefik '971 and Stefik '392, with a binary

Art Unit: 2132

tree hierarchy of Aiello in order to reduce the consequent number of tokens (keys) needed to be updated each time a user's key is invalidated in a hierarchical structure (*see* Aiello col. 10 ll. 48-56), thus assuring low-overhead billing, and the convenience of access, despite some unauthorized copying (*see* Stefik '971, col. 15 ll. 15-25).

30. **Regarding (new) claim 17:** The combination of Sweet, Stefik '971 and Stefik '392 discloses a method as indicated above, wherein the security keys are ancestry based (Stefik '971, col. 11-12 ll. 59-3).

The combination of Sweet, Stefik '971 and Stefik '392 does not describe wherein the security keys are generated in an ancestry-based, binary tree hierarchy, wherein invalidation of a given key necessitates a need for reconfiguration of each key in the hierarchy, or wherein the value for economic disbenefit to the provider is computed by adding a first cost associated with invalidating the ineligible user's security key, with a second cost associated with reconfiguring all security keys of eligible users that are in an upper ancestry level in a same ancestry chain as the ineligible user's security key, and with a third cost associated with invalidating all security keys in the binary tree hierarchy that are of a lower ancestry level in the same ancestry chain as the ineligible user's security key.

Aiello describes wherein the security keys are generated in an ancestry-based, binary tree hierarchy (col. 8 ll. 52),

wherein invalidation of a given key necessitates a need for reconfiguration of each key in the hierarchy (col. 6-7 ll. 10-4, token value dependent on chain),

wherein the value for economic disbenefit to the provider is computed by adding a first cost associated with invalidating the ineligible user's security key, with a second cost associated with reconfiguring all security keys of eligible users that are in an upper ancestry level in a same ancestry chain as the ineligible user's security key, and with a third cost associated with invalidating all security keys in the binary tree hierarchy that are of a lower ancestry level in the same ancestry chain as the ineligible user's security key (col. 5-7 ll. 55-63, cost of communications and network resources reduced by selected revocation and updating scheme in binary tree structure using chain of token values).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the combination of Sweet, Stefik '971 and Stefik '392, with a binary tree hierarchy of Aiello in order to reduce the consequent number of tokens (keys) needed to be updated each time a user's key is invalidated in a hierarchical structure (*see* Aiello col. 10 ll. 48-56), thus assuring low-overhead billing, and the convenience of access, despite some unauthorized copying (*see* Stefik '971, col. 15 ll. 15-25).

**31. Claims 18 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Sweet and Stefik '971.**

**32. Regarding (new) claims 18 and 19:** The combination of Sweet and Stefik '971 discloses a method as indicated above, wherein the issuing step is performed by a server, and wherein the issuing step includes providing the security key to the first user in a cookie returned to the first user by the server over the Internet (Sweet, [0281] cookie).

Art Unit: 2132

33. **Claims 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Sweet, Stefik '971 and Aiello.**

34. **Regarding (new) claims 20 and 21:** The combination of Sweet, Stefik '971, Stefik '392, and Aiello discloses a method as indicated above, wherein the second and third costs include a cost associated with creating a new binary tree to provide a new set of security keys to replace all invalidated security keys (Aiello, col. 5-7 ll. 55-63).

***Repeated Claim Rejections***

***Claim Rejections - 35 USC § 103***

35. Claims [[1 and]] 10- 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sweet et al. (US PGPub 2002/0031230 A1), in view of Stefik et al. (US Patent #6,236,971 ).

Here, Sweet clearly shows the use of a method of managing security keys (see paragraph 0023) provided to users of a service comprising the steps of: issuing a security key to a first user eligible to receive the service (see paragraph 0037); monitoring the first user's status to establish whether the first user is eligible to receive the service (see paragraph 0025). However, Sweet does not teach the use of an establishment, in accordance with a policy, of a first value associated with invalidation of the first user's key, and a second value associated with providing the service to an ineligible user, and if the second value exceeds the first value, invalidating the key.

On the other, hand, Stefik does teach the use of establishing a policy using repository security classes which can create and manage such values mentioned above (see column 14, lines 34 - 40).

Art Unit: 2132

Hence, it would have been obvious to one of ordinary skill in the art to have included the technology shown by Stefik into the device taught by Sweet above, in order to assure the convenience of access and low-overhead billing, despite some unauthorized copying (see column 15, lines 15 - 25 of the Stefik reference). With respect to claims 10-12, their limitations map directly onto the ones shown in claim land are rejected under the same premise.

36. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sweet in view of Stefik '971 as applied to claims 1 and 10 - 12 above, and further in view of Aiello. The Sweet and Stefik '971 references have already been discussed above. However, neither one of these two teaches a policy that further provides the first value as related to the economic penalty associated with reconfiguration of keys issued to other users consequent to invalidation of the first user's key.

On the other hand, Aiello does teach the use of a key invalidation scheme (i.e. policy) that provides the first value as related to the economic penalty associated with reconfiguration of keys issued to other users consequent to invalidation of the first user's key (see col. 11 -12, ll. 36 - 67 and 1 - 26).

Hence, it would have been obvious to one of ordinary skill in the art to have included the methods shown by Aiello into the combination taught by prior two references above, in order to reduce the consequent number of tokens (keys) needed to be updated each time a user's key is invalidated in a hierarchical structure (*see* Aiello col. 10 ll. 48-56), thus assuring low-overhead billing, and the convenience of access, despite some unauthorized copying (*see* Stefik '971, col. 15 ll. 15-25).



37. Claim [[s 3 -]] 4 [[are]] is rejected under 35 U.S.C. 103(a) as being unpatentable over Sweet et al. (US PGPub 2002/0031230 A1) in view of Stefik et al. (US Patent #7,024,392 B2).

The Sweet reference has already been discussed above. However, the Sweet reference does not teach the use of a policy which provides the second value as related to aggregating the economic penalty associated with provision of the service to the ineligible user.

On the other hand, Stefik does teach the use of a policy using repository security classes which can create and calculate such a value as described above (see column 14, lines 20 - 25 and 34 - 40).

Hence, it would have been obvious to one of ordinary skill in the art to have included the technology shown by Stefik into the device taught by Sweet above, in order to help ensure the convenience of access and low-overhead billing, despite some unauthorized copying (see column 15, lines 15 - 25 of the Stefik reference). With respect to claim 3, the limitations shown there map directly onto the ones shown in claim 4 and are rejected under the same premise.

38. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sweet et al. (US PGPub 2002/0031230 A1) in view of Stefik et al. (US Patent # 7,024,392 B2). The Sweet reference has already been discussed above. However, the Sweet reference does not teach the use of an economic penalty associated with provision of service to ineligible users, including a value representative of dilution of economic value to eligible users consequent to provision of the service to ineligible users.

On the other hand, Stefik does teach the use of a policy using repository security classes which can create and calculate such a value as described above (see column 6, lines 15 - 30, and column 14, lines 20 - 25 and 34 - 40).

Hence, it would have been obvious to one of ordinary skill in the art to have included the technology shown by Stefik into the device taught by Sweet above, in order to help ensure the convenience of access and low-overhead billing, despite some unauthorized copying (see column 15, lines 15 - 25 of the Stefik reference).

39. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sweet et al. (US PGPub 2002/0031230 A1) in view of Stefik et al. (US Patent # 7,024,392 B2). The Sweet reference has already been discussed above. However, the Sweet reference does not teach the use of an economic penalty of providing the service to ineligible users, including any costs arising from the provision of network and server capacity to ineligible users.

On the other hand, Stefik does teach the use of a policy using repository security classes which can create and calculate such a value as described above (see column 6, lines 15 - 20, and column 14, lines 20 - 25 and 34 - 40).

Hence, it would have been obvious to one of ordinary skill in the art to have included the technology shown by Stefik into the device taught by Sweet above, in order to help ensure the convenience of access and low-overhead billing, despite some unauthorized copying (see column 15, lines 15 - 25 of the Stefik reference).

Art Unit: 2132

40. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sweet et al. (US PGPub 2002/0031230 A1) in view of Stefik et al. (US Patent # 6,236,971) as applied to claims 1 and 10 - 12 above, and further in view of Aiello et al. (US Patent# 6,397,329 B1). The Sweet and Stefik references have already been discussed above. However, neither one of these two teaches the use of security keys being generated in an ancestrally-based hierarchy, and wherein invalidation of a given key necessitates a need for reconfiguration of each key in the hierarchy.

On the other hand, Aiello does teach the use of security keys being generated in an ancestrally-based hierarchy (see column 8, lines 35 - 60), and wherein invalidation of a given key necessitates a need for reconfiguration of each key in the hierarchy (see columns 13- 14, lines 39-67 and 1 -31).

Hence, it would have been obvious to one of ordinary skill in the art to have included the methods shown by Aiello into the combination taught by prior two references above, in order to reduce the consequent number of tokens (keys) needed to be updated each time a user's key is invalidated in a hierarchical structure (see columns 5 and 10, lines 55 - 60 and 48 - 56 of the Aiello reference), thus assuring low-overhead billing and the convenience of access, despite some unauthorized copying (see column 15, lines 15 - 25 of the Stefik reference).

41. Claims 8 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sweet et al. (US PGPub 2002/0031230 A1) in view of Stefik et al. (US Patent # 6,236,971) as applied to claims 1 and 10 - 12 above, and further in view of Aiello et al. (US Patent # 6,397,329 B1). The Sweet and Stefik references have already been discussed above. However, neither one of these

Art Unit: 2132

two teaches that upon invalidation of a given key, another key requires reconfiguration only to the extent that it shares common ancestor keys with the given invalidated key.

On the other hand, Aiello does teach that upon invalidation of a given key, another key requires reconfiguration only to the extent that it shares common ancestor keys with the given invalidated key (see columns 10, lines 19-48).

Hence, it would have been obvious to one of ordinary skill in the art to have included the methods shown by Aiello into the combination taught by prior two references above, in order to reduce the consequent number of tokens (keys) needed to be updated each time a user's key is invalidated in a hierarchical structure (see columns 5 and 10, lines 55 - 60 and 48 - 56 of the Aiello reference), thus assuring low-overhead billing and the convenience of access, despite some unauthorized copying (see column 15, lines 15 - 25 of the Stefik reference). With respect to claim 13, the limitations shown there map directly onto the ones shown in claim 8 and are rejected under the same premise.

42. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sweet et al. (US PGPub 2002/0031230 A1) in view of Stefik et al. (US Patent # 6,236,971) as applied to claims 1 and 10 - 12 above, and further in view of Aiello et al. (US Patent # 6,397,329 B1). The Sweet and Stefik references have already been discussed above. However, neither one of these two teaches the use of a binary tree as the hierarchy.

On the other hand, Aiello does teach the use of a binary tree as the hierarchy (see column 8, lines 34 - 36).

Art Unit: 2132

Hence, it would have been obvious to one of ordinary skill in the art to have included the methods shown by Aiello into the combination taught by prior two references above, in order to reduce the consequent number of tokens (keys) needed to be updated each time a user's key is invalidated in a hierarchical structure (see columns 5 and 10, lines 55 - 60 and 48 - 56 of the Aiello reference), thus assuring low-overhead billing and the convenience of access, despite some unauthorized copying (see column 15, lines 15 - 25 of the Stefik reference).

### *Conclusion*

43. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is:

- Hollar, U.S. Patent No. 7,124,114 B1, regarding economic penalty for provision to unauthorized user.

44. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2132

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Please direct any inquiry concerning this communication or earlier communications from the examiner to Bea Koempel-Thomas whose telephone number is 571-270-1252. The examiner can normally be reached on Monday - Thursday & alternate Fridays; 0730 - 1700.

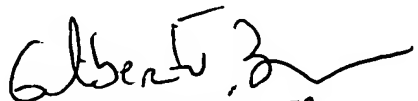
If attempts to reach the examiner by telephone are unsuccessful, please contact the examiner's supervisor, Gilberto Barron, at 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Bea Koempel-Thomas, Esq.  
Patent Examiner  
AU 2132



3/8/2007

  
GILBERTO BARRON JR  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100